Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for allowing a financial transaction to be performed using a electronic system, the method comprising:

interrogating an electronic transaction terminal with an electronic security device to obtain an integrity metric for the ~~electronic~~ transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal~~, the integrity metric indicative of at least one operating variable associated with the electronic transaction terminal~~;

determining if the transaction terminal is a trusted terminal based upon the integrity metric; and

allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal.

2. (previously presented) A method according to claim 1, further comprising:

providing user identification data for the user of the electronic security device to the transaction terminal via the security device to allow authorisation of the transaction associated with the financial transaction data.

3. (previously presented) A method according to claim 1, further comprising:

displaying a user secret if the transaction terminal is identified as a trusted terminal.

4. (previously presented) A method according to claim 1, further comprising:

compartmenting different types of transactions into different compartments.

5. (currently amended) A financial transaction system, comprising:

an electronic financial transaction terminal; and

an electronic security device having interrogation means for interrogating the ~~electronic financial~~ transaction terminal to obtain an integrity metric for the ~~electronic financial~~ transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal ~~indicative of at least one operating variable associated with the electronic financial transaction terminal~~, determining means for determining if the transaction terminal is a trusted terminal based upon the integrity metric, and means for allowing financial transaction data to be input into the transaction terminal if the transaction terminal is

identified as a trusted terminal.

6. (original) A financial transaction system according to claim 5, wherein the electronic financial transaction terminal further comprises a display for displaying a user secret if the transaction terminal is identified as a trusted terminal.

7. (original) A financial transaction system according to claim 6, wherein the user secret is deleted on completion of the financial transaction.

8. (currently amended) An electronic security transaction device having interrogation means for interrogating an electronic financial transaction terminal to obtain an integrity metric for the ~~electronic financial~~ transaction terminal measured by a trusted device associated with the transaction terminal after the last restart of the transaction terminal ~~indicative of at least one operating variable associated with the electronic financial transaction terminal~~, determining means for determining if the transaction terminal is a trusted terminal based upon the integrity metric, and means for allowing financial transaction data to be input into the transaction terminal if the transaction terminal is identified as a trusted terminal.

9. (original) An electronic security transaction device

according to claim 8, further comprising a switch for initiating the transfer of financial transaction data to the transaction terminal if the transaction terminal is identified as a trusted terminal.

10. (original) An electronic security transaction device according to claim 8, wherein the transaction device is a wireless trusted personnel device.

11. (withdrawn) A method, comprising:

controlling boot-up of a computing platform with a trusted process to acquire a value for at least one integrity metric indicative of an operating variable associated with the platform, the trusted process implemented to be inaccessible by other software executable on the platform;

receiving a request for determining whether the platform may be trusted to conduct a transaction; and

responding to the request by providing the acquired value for the integrity metric and an authenticated value for the integrity metric, the authenticated value obtained from a source separate from the platform.

12. (withdrawn) The method of claim 11, wherein controlling boot-up comprises:

determining whether the trusted process was the first

process accessed by the computing platform upon initiation of boot-up.

13. (withdrawn) The method of claim 11, wherein controlling boot-up comprises:

computing a digest of a BIOS memory of the computing platform to acquire the integrity metric value.

14. (withdrawn) The method of claim 11, wherein controlling boot-up comprises:

computing a digest of each of a plurality of functional blocks within a BIOS memory of the computing platform; and

computing a digest of the digests computed for the plurality of functional blocks to acquire the integrity metric value.

15. (withdrawn) The method of claim 11, wherein controlling boot-up comprises:

issuing fixed challenges to one or more components of the computing platform; and

receiving responses to the challenges to acquire the integrity metric value.

16. (withdrawn) The method of claim 11, wherein controlling boot-up comprises:

passing control of the computing platform to a BIOS memory of the platform only if a computed digest of the BIOS memory matches the authenticated integrity metric value.

17. (withdrawn) The method of claim 12, wherein controlling boot-up comprises:

passing control of the computing platform to a BIOS memory of the platform only if the trusted process was the first process accessed by the computing platform upon initiation of boot-up.